(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 June 2003 (12.06.2003)

PCT

(10) International Publication Number
WO 03/049357 A3

(51) International Patent Classification[7]: H04L 29/06, 12/22, 9/32

(21) International Application Number: PCT/EP02/14080

(22) International Filing Date: 6 December 2002 (06.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0129339.8 7 December 2001 (07.12.2001) GB
0104283-7 18 December 2001 (18.12.2001) SE

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; SE-12625, S- STOCKHOLM (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **UUSITALO, Ilkka** [FI/FI]; Palosuontie 6 b 6, FIN-90800 Oulu (FI). **AHONEN, Pasi** [FI/FI]; Salotie 5, FIN-90630 Oulu (FI). **BLOM, Rolf** [SE/SE]; Svardvagen 2, SE-17568 Jarfalla (SE). **BOMAN, Krister** [SE/SE]; Idunagatan 2, SE-43144 Molndal (SE). **NÄSLUND, Mats** [SE/SE]; Grimstagatan 161, SE-16258 Vällingby (SE).

(74) Agents: **LIND, Robert** et al.; Marks & Clerk, 4220 Nash Court, Oxford Business Park South, Oxford, Oxfordshire OX4 2RU (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

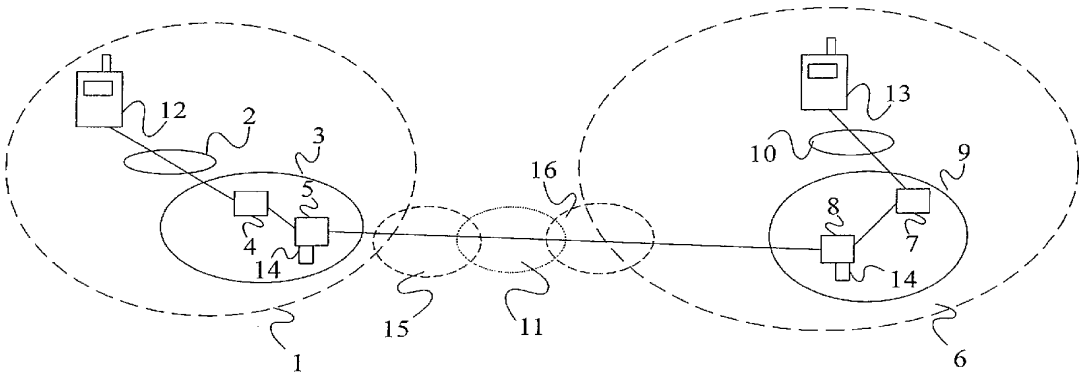
Published:
— *with international search report*
— *with amended claims*

(88) Date of publication of the international search report: 9 October 2003

Date of publication of the amended claims: 27 November 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: LAWFUL INTERCEPTION OF END-TO-END ENCRYPTED DATA TRAFFIC



(57) Abstract: A method of facilitating the lawful interception of an IP session between two or more terminals 12,13, wherein said session uses encryption to secure traffic. The method comprises storing a key allocated to at least one of said terminals 12,13 or to at least one of the subscribers using one of the terminals 12,13, at the terminal 12,13 and at a node 5,8 within a network 1,6 through which said session is conducted, or a node coupled to that network. Prior to the creation of said session, a seed value is exchanged between the terminal 12,13 at which the key is stored and said node 5,8. The key and the seed value are used at both the terminal 12,13 and the node 5,8 to generate a pre-master key. The pre-master key becomes known to each of the terminals 12,13 involved in the IP session and to the network node 5,8. The pre-master key is used, directly or indirectly, to encrypt and decrypt traffic associated with said IP session.

WO 03/049357 A3

AMENDED CLAIMS
[received by the International Bureau on 8 August 2003 (08.08.03);
original claims 1, 15 and 16 amended; remaining claims unchanged (2 pages)]

1. A method of facilitating the lawful interception of a data session between two or more terminals, wherein said session uses encryption to secure traffic, the method comprising:

storing a key allocated to at least one of said terminals, at the terminal and at a node within a network through which said session is conducted or at a node coupled to that network;

prior to the communication of a session setup request from the calling terminal to the called terminal exchanging a seed value between the terminal at which the key is stored and said node;

using the key and the seed value at the terminal to generate a pre-master key, wherein the pre-master key subsequently also becomes known to the or each other terminal involved in the data session; and

directly or indirectly using said pre-master key to encrypt and decrypt traffic associated with said session.

2. The method of claim 1, wherein said node generates the pre-master key for use in lawful interception of the data session.

3. The method of claim 1 or 2, wherein said step of using the key and the seed value at the terminal to generate a pre-master key comprises using a key exchange procedure to transmit a first cross-parameter from the said at least one terminal to another terminal and to transmit a second cross-parameter from that other terminal to the said at least one terminal.

4. The method of claim 3, wherein said key exchange procedure is a Diffie-Hellman exchange.

5. The method of claim 4, and comprising applying a key derivation function to said key and the seed value to derive a second key, an exponentiation of the second key then being generated for use in the Diffie-Hellman exchange.

a second key sent to the at least one terminal from a peer terminal during the Diffie-Hellman exchange, and generating the pre-master key using that detected exponentiated second key and the second key of the said at least one terminal.

15. A subscriber module for use in a communication terminal, the module comprising:

a memory for storing a key allocated to a subscriber using the terminal;

means for exchanging a seed value between the module and a node of a communications network over which an encrypted data session is to be conducted or a node coupled to that network, prior to the communication of a session setup request between the communicating terminals;

means for using the key and the seed value to generate a pre-master key which pre-master key also becomes known to the or each other terminal involved in the data session; and

means for directly or indirectly using the pre-master key to encrypt and decrypt traffic associated with said session.

16. A network node for use in intercepting encrypted traffic associated with a data session conducted between two or more terminals coupled to a communications network, the node comprising:

a memory storing keys allocated to terminals or subscribers registered with the network;

means for exchanging seed values with terminals prior to the communication of a session setup request between terminals and the setting up of a data session between the terminals; and

means for using the key and the seed value to generate a pre-master key or for passing the key and seed value to another node having means for using the key and the seed value to generate a pre-master key.

17. A method of facilitating the lawful interception of a data session between two or more terminals, wherein said session uses encryption to secure traffic and at least one of the terminals is a mobile wireless device, the method comprising:

storing a key allocated to said at least one terminal or to a subscriber, at the terminal and at a node within the terminal's/subscriber's home network;